AF # 2161

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Edenson et al.	Docket No.:	TI-25667
Serial No.:	09/170,864	Art Unit:	2161
Filed:	10/13/1998	Examiner:	Elisca, Pierre
For:	SECURE DISTRIBUTION OF DIGITAL DATA		

APPEAL BRIEF TRANSMITTAL

May 2, 2002

Assistant Commissioner for Patents
Washington, D. C. 20231

MAILING CERTIFICATE UNDER 37 C.F.R. §1.8(A)
I hereby certify that the above correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to: Assistant Commissioner For Patents, Washington, D.C. 20231 on the date below.

Charles A. Brill — 2 May 2002
Charles A. Brill — Date

Sir:

Transmitted herewith in triplicate is an Appeal Brief in the above-identified application.

Please charge the $320.00 fee for filing the Brief to the deposit account of Texas Instruments Incorporated, Account No. 20-0668.

Charge any additional fees, including any extension of time fees, or credit overpayment to the deposit account of Texas Instruments Incorporated, Deposit Account No. 20-0668. An original and two copies of this sheet are enclosed.

Respectfully submitted,

Charles A. Brill
Attorney for Applicant(s)
Reg. No. 37,786

Texas Instruments Incorporated
P. O. Box 655474, MS 3999
Dallas, Texas 75265
Telephone: (972) 917-4379
Fax: (972) 917-4418

#14 NG

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Edenson et al.	Art Unit:	2161
Serial No.:	09/170,864	Examiner:	Elisca, Pierre
Filed:	10/13/1998	Docket No.:	TI-25667

For: SECURE DISTRIBUTION OF DIGITAL DATA

COPY OF PAPERS ORIGINALLY FILED

APPEAL BRIEF UNDER 37 C.F.R. § 1.192

May 2, 2002

Assistant Commissioner for Patents
Washington, D.C. 20231

MAILING CERTIFICATE UNDER 37 C.F.R. 31.8(A)
I hereby certify that the above correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on the date shown below.

Charles A. Brill — 2 May 2002
Charles A. Brill — Date

Dear Sir:

The following Appeal Brief is respectfully submitted, in triplicate, in connection with the above-identified application in response to the Final Rejection mailed November 26, 2001, and the Advisory Action mailed March 8, 2002. Please charge all required fees, including any extension of time fees, to the deposit account of Texas Instruments Incorporated, Deposit Account Number 20-0668.

REAL PARTY IN INTEREST

The real party in interest is Texas Instruments Incorporated, to whom this application is assigned.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to the Applicant's legal representative.

STATUS OF THE CLAIMS

This application was originally filed with forty-two claims, five of which were written in independent form. Claims 1-24 have been allowed. Claims 25-42 have been rejected.

STATUS OF THE AMENDMENTS

No claims have been amended during the prosecution of this application. A response to the final rejection was filed 19 February 2002, but did not propose amendments to the claims.

SUMMARY OF THE INVENTION

The abstract contains a brief summary of the present invention. Digital data is stored on digital storage media and authorization data is stored on an identification system module. The authorization data describes which media players are authorized to read the storage media. The invention also provides for collecting and tracking information concerning the usage of the stored data.

One application of the invention is the creation of media storing movies for theatrical release. In this application, the studio could encrypt and store video data on the media and store authorization data in an associated identification system module prior to shipping the media to a theater (page 11, line 10 to page 12, line 7). In use, a media player at an authorized theater would read the authorization data from the identification system and determine the media player was authorized to read the data, and read the data from the storage media (page 12, line 18 to page 13, line 22). The media player additionally could store information in the identification system module for later readout (page 16, line 3 to page 17, line 3).

ISSUES

1. Whether Claims 25-42 are anticipated under 35 U.S.C. § 102 (e) by U.S. Patent No. 5,790,674 to Houvener et al. ("Houvener").

GROUPING OF THE CLAIMS

Claims 25-27 and 29-42 are each independently patentable over the prior art of record and should be deemed to stand or fall individually for the reasons more clearly set forth hereinbelow. Claim 28 is a duplicate of Claim 27 and should be withdrawn. Claims 41 and 42 are duplicates of Claim 40 and should be withdrawn.

ARGUMENTS

Issue 1:

Claims 25-42 were rejected as being anticipated under 35 U.S.C. § 102 (e), or according to the Office Action mailed November 26, 2001 under §102(a), as being anticipated by Houvener. The applicant respectfully disagrees.

"A person shall be entitled to a patent unless," creates an initial presumption of patentability in favor of the applicant. 35 U.S.C. § 102. "We think the precise language of 35 U.S.C. § 102 that, "a person shall be entitled to a patent unless," concerning novelty and unobviousness, clearly places a burden of proof on the Patent Office which requires it to produce the factual basis for its rejection of an application under sections 102 and 103, see Graham and Adams." *In re Warner*, 379 F.2d 1011, 1016 (C.C.P.A. 1967) (referencing *Graham v. John Deere Co.*, 383 U.S. 1 (1966) and *United States v. Adams*, 383 U.S. 39 (1966)). "As adapted to *ex parte* procedure, *Graham* is interpreted as continuing to place the 'burden of proof on the Patent Office which requires it to produce

the factual basis for its rejection of an application under sections 102 and 103'." *In re Piasecki*, 745 F.2d 1468 (Fed. Cir. 1984).

"The prima facie case is a procedural tool which, as used in patent examination (as by courts in general), means not only that the evidence of the prior art would reasonably allow the conclusion the examiner seeks, but also that the prior art compels such a conclusion if the applicant produces no evidence or argument to rebut it." *In re Spada*, 911 F.2d 705, 708 n.3 (Fed. Cir. 1990).

The applicant respectfully submits the Examiner has failed to meet the burden of proof required to establish a *prima facie* case of anticipation. Section 2131 of the Manual of Patent Examiner's Procedure provides:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053, (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as contained in the . . . claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim . . . . *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

With respect to independent claim 25, the applicant has asserted Houvener fails to teach "an identification system module . . . containing an authorization code describing which media players are authorized to read digital data from said digital storage medium" as recited by Claim 25. The Examiner has responded "this limitation is disclosed by Houvener in col 4, lines 1-12, col 6, lines 54-67, specifically wherein it is stated that at

the point of identification terminal (or identification system module) and [sic] searches the database to find the unique image (or media players) data corresponding to the unique data."

The cited passage in column 4 of Houvener states:

At the database site, the system receives the information presented at the point of identification terminal and searches the database to find the unique image data corresponding to the unique data. The system then transmits the image data to the point of identification terminal where it is displayed on a display means. Finally, the system incorporates a means for verifying that an identifier present at the point of verification has adequately verified that the digital image displayed on the display means matches physical or biometric information provided by the person to be identified at the point of identification terminal."

The cited passage in column 6 of Houvener states:

The identifier, which would be the sales clerk in a retail establishment, would only need to input the credit card information into one device and would receive both credit approval and identity verification from a single source. In this scenario, input/output controller 13 would initiate a credit authorization request to an outside CAA 23 through modem bank 14 over public access telephone lines 12 or through a WAN connection 14' or the like. If the amount of the transaction is approved by the CAA 23, the database site would receive the credit approval code from the CAA and retransmit the code to the point of verification terminal along with the digital image information or other unique data over its established communications link. The credit approval code would be displayed either on the

display means 6 of the point of verification terminal or, in the alternative, on an optional second display means 6'.

The Examiner appears to equate the use of a terminal to read a credit card and pass information from the credit card to a remote database, to receive credit approval and identification image data from the remote database with the claimed limitation of an "identification system module containing an authorization code describing which media players are authorized to read digital data from said digital storage medium." These passages simply do not support the Examiner's transformation of the teachings of Houvener to the recited elements of Claim 25, nor is there any basis or suggestion in the prior art to support this novel interpretation of the prior art. The Examiner's rejection is unsuppcrted by the prior art, fails to establish a prima facie case of anticipation, and therefore should be withdrawn.

Claim 26 depends from Claim 25 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 25, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 26—e.g. "said digital storage medium comprising an optical disc."

Claim 27 depends from Claim 25 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 25, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 27—e.g. "said identification system module comprising a TIRIS transponder."

Claim 29 depends from Claim 25 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 25, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 29—e.g. "said identification system stores usage information."

Claim 30 depends from Claim 25 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 25, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 30—e.g. "said usage information comprises information concerning the number for time [sic] said digital data has been read."

Claims 31 and 38 are independent claims respectively reciting a method of securely distributing digital data, and a method of tracking the use of information. As argued above, the Examiner has the burden of establishing a *prima facie* case of anticipation. The applicant suggests the Examiner has failed to meet this burden.

The Examiner has not addressed the method limitations of independent claims 31 and 38, but instead merely states, "Regarding to claims 31 and 32, the claimed invention have the similar limitations as claim 25 and therefore the same rejection applied." With respect to Claim 31, the Examiner has not addressed the limitation of "transferring said digital storage media to a user," nor does there appear to be any "similar limitation" in Claim 25 as suggested by the Examiner. With respect to Claim 38, the Examiner has not addressed the limitations of "storing usage information concerning said reading step on said storage media" or "transmitting said information to an information collection

agency," nor do there appear to be any "similar limitation" in Claim 25 as suggested by the Examiner.

Claim 32 depends from Claim 31 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 31, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim ~~30~~ 32 CB—e.g. "writing digital data onto an optical disc."

Claim 33 depends from Claim 31 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 31, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 33—e.g. "attaching an RF identification system to said digital storage medium."

Claim 34 depends from Claim 31 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 31, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 34—e.g. "attaching a TIRIS responder to said digital storage medium."

Claim 35 depends from Claim 31 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 31, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 35—e.g. "adding a digital watermark to said digital data; and wherein said step of writing digital data onto

a digital storage medium comprises the step of writing said digital data containing said digital watermark onto said digital storage medium."

Claim 36 depends from Claim 31 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 31, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 36—e.g. "reading said digital data from said digital storage medium; and storing usage information on said digital storage medium."

Claim 37 depends from Claim 31 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 31, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 37—e.g. "reading said digital data from said digital storage medium; and transmitting usage information to a collection agency."

Claim 39 depends from Claim 38 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claim 38, the Examiner has not made any attempt to read Houvener on the additional limitations recited by Claim 39—e.g. "storing usage information concerning said reading step in an identification system module attached to said storage media."

Claim 40 depends from Claim 39 and should be deemed allowable for that reason and on its own merits. Not only has the Examiner failed to establish a *prima facie* case of anticipation, as argued above with respect to Claims 38 and 39, the Examiner has not

made any attempt to read Houvener on the additional limitations recited by Claim 40—e.g. "transferring said identification system to a distributor."

CONCLUSION

For the foregoing reasons, Appellants respectfully submit that the Examiner's final rejection of Claims 25-42 under 35 U.S.C. § 102 as being anticipated by Houvener is improper, and it is respectfully requested that the Board of Patent Appeals and Interferences so find and reverse the Examiner's rejection.

Please charge any fees necessary in connection with the filing of this paper, including any necessary extension of time fees, to Deposit Account No. 20-0668 of Texas Instruments Incorporated.

Respectfully submitted,

Charles A. Brill
Attorney for Applicant
Reg. No. 37,786

Texas Instruments Incorporated
P.O. Box 655474 M/S 399
Dallas, TX 75265
(972) 917-4379
FAX: (972) 917-3511

APPENDIX

1. A secure digital image projection system having at least one identification code identifying said image projection system, said image projection system comprising:

an identification system interrogator for reading an authorization code from an identification system module associated with a data storage medium;

a verification unit for verifying said authorization code matches said identification code;

a media player for reading digital data stored on said data storage medium; and

a projection unit for displaying said digital data on the condition that said authorization code matches said identification code.

2. The secure digital image projection system of Claim 1, said identification system module comprising an RF identification system module.

3. The secure digital image projection system of Claim 1, said identification system module comprising a TIRIS transponder.

4. The secure digital image projection system of Claim 1, wherein said digital data stored on said medium is encrypted, said projection system further comprising:

a decryption unit for decrypting said encrypted digital data prior to display of said digital data.

5. The secure digital image projection system of Claim 1, said image projection system further comprising:

a media jukebox for opening a tamper-proof cartridge containing said data storage medium, and for accessing said data storage medium.

6. The secure digital image projection system of Claim 1, wherein said projection system adds a digital watermark to said digital data read from said data storage medium.

7. The secure digital image projection system of Claim 1, wherein said media player adds a digital watermark to said digital data read from said data storage medium.

8. The secure digital image projection system of Claim 1, wherein said projection unit adds a digital watermark to said digital data read from said data storage

medium.

9. The secure digital image projection system of Claim 1, wherein said projection system stores usage information on said identification system module.

10. The secure digital image projection system of Claim 9, wherein said usage information comprises at least one said identification code identifying said image projection system.

11. The secure digital image projection system of Claim 1, wherein said projection system transmits usage information to a collection agency.

12. The secure digital image projection system of Claim 11, wherein said usage information comprises at least one said identification code identifying said image projection system.

13. The secure digital image projection system of Claim 1:

said media player having a first identification code;

said projector unit having a second identification code; and

said verification unit comprising a first verification unit in said media player and a second verification unit in said projector unit, said authorization code comprising a first and a second authorization code, said media player only reading said digital data from said data storage medium on the condition that said first authorization code matches said first identification code, and said projector unit only displaying said digital data on the condition that said second authorization code matches said second identification code.

14. A secure digital data media player comprising:

an identification system interrogator for reading authorization information from an identification system module attached to a digital data storage medium and verifying said authorization information authorizes said media player to read said digital data storage medium; and

a media reader for reading data from said digital data storage medium and outputting said data on the condition said authorization information authorizes said media player to read said digital data storage medium.

15. The secure digital data media player of Claim 14, said identification system module comprising an RF identification system module.

16. The secure digital data media player of Claim 14, said identification system module comprising a TIRIS transponder.

17. The secure digital data media player of Claim 14, wherein said digital data stored on said medium is encrypted, said media player-projector further comprising:

a decryption unit for decrypting said encrypted digital data prior to display of said digital data.

18. The secure digital data media player of Claim 14, further comprising:

a media jukebox for opening a tamper-proof cartridge containing said data storage medium, and for accessing said data storage medium.

19. The secure digital data media player of Claim 14, wherein said media player adds a digital watermark to said data read from said digital data storage medium.

20. The secure digital data media player of Claim 14, wherein said media player adds a digital watermark to said data read from said digital data storage medium.

21. The secure digital data media player of Claim 14, wherein said projection system stores usage information on said identification system module.

22. The secure digital data media player of Claim 21, wherein said usage information comprises at least one said identification code identifying said secure digital data media player.

23. The secure digital data media player of Claim 14, wherein said projection system transmits usage information to a collection agency.

24. The secure digital data media player of Claim 23, wherein said usage information comprises the at least one said identification code identifying said secure digital data media player.

25. A secure data storage medium comprising:

a digital storage medium for storing digital data; and

an identification system module corresponding to said digital storage medium, said identification system module containing an authorization code describing which media players are authorized to read digital data from said digital storage medium.

26. The secure data storage medium of Claim 25, said digital storage medium comprising an optical disc.

27. The secure data storage medium of Claim 25, said identification system module comprising a TIRIS transponder.

28. The secure data storage medium of Claim 25, said identification system module comprising a TIRIS transponder.

29. The secure data storage medium of Claim 25, wherein said identification system stores usage information.

30. The secure data storage medium of Claim 29, wherein said usage information comprises information concerning the number of time said digital data has been read.

31. A method of securely distributing digital data, said method comprising:

writing digital data onto a digital storage medium;

attaching an identification system module to said digital storage medium, said identification system module containing an authorization code indicating which media readers are authorized to read said digital storage medium; and

transferring said digital storage medium to a user.

32. The method of Claim 31, said writing step comprising the step of writing digital data onto an optical disc.

33. The method of Claim 31, said attaching step comprising the step of attaching an RF identification system to said digital storage medium.

34. The method of Claim 31, said attaching step comprising the step of attaching a TIRIS responder to said digital storage medium.

35. The method of Claim 31, further comprising the step of:

adding a digital watermark to said digital data; and

wherein said step of writing digital data onto a digital storage medium comprises the step of writing said digital data containing said digital watermark onto said digital storage medium.

36. The method of Claim 31, further comprising the step of:

reading said digital data from said digital storage medium; and

storing usage information on said digital storage medium.

37. The method of Claim 31, further comprising the step of:

reading said digital data from said digital storage medium; and

transmitting usage information to a collection agency.

38. A method of tracking the use of information, said method comprising:

storing said information on storage media;

reading said information;

storing usage information concerning said reading step on said storage media; and

transmitting said information to an information collection agency.

39. The method of Claim 38 wherein said storing usage information step comprises:

storing usage information concerning said reading step in an identification system module attached to said storage media.

40. The method of Claim 39 wherein said transmitting said information step comprises:

transferring said identification system to a distributor.

41. The method of Claim 39 wherein said transmitting said information step comprises:

transferring said identification system to a distributor.

42. The method of Claim 39 wherein said transmitting said information step comprises:

transferring said identification system to a distributor.